

CLAIMS:

1. A method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method
5 comprising:
 - generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space;
 - transmitting the plurality of random quantum states of the quantum entity via
10 the quantum channel to the recipient;
 - measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space;
 - transmitting to the recipient composition information describing a subset of the
15 plurality of random quantum states;
 - analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;
 - 20 establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;
 - deriving a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum
25 states not in the subset; and
 - carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings.
- 30 2. A method according to Claim 1, wherein the first and second plurality of bases in Hilbert space each comprise at least four random bases.

3. A method according to Claim 1, wherein the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space.
4. A method according to Claim 1, wherein the selecting step comprises
5 generating and measuring a first plurality of bases in a real subspace of two-dimensional Hilbert space.
5. A method according to Claim 1, wherein the composition information transmitting step comprises transmitting information describing the bases of the subset
10 of the plurality of random quantum states.
6. A method according to Claim 1, wherein the analysing step comprises analysing the information describing the bases to derive the first statistical distribution.
15
7. A method according to Claim 1, wherein the establishing step comprises determining a statistical error rate.
8. A method according to Claim 1, wherein the establishing step comprises:
20 determining the degree of difference between the first and second statistical distributions; and
accepting the security of the channel if the degree of correlation between the two distributions is greater than a threshold level.
9. A method according to Claim 8, further comprising selecting the value of the
25 threshold level.
10. A method according to Claim 1, wherein the subset information transmitting step comprises transmitting the subset information over a public channel, such as a
30 radio channel.

11. A method according to Claim 1, wherein the deriving step comprises transmitting information to the recipient representing the bases for the quantum states not in the subset which make up the first binary string.
- 5 12. A method according to Claim 1, wherein the carrying out the reconciliation step comprises using privacy amplification techniques.
13. A method according to Claim 1, wherein the quantum entity is photons and the quantum states are degrees of polarisation of the photons.
- 10 14. A method according to Claim 1, further comprising temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step.
- 15 15. A method according to Claim 14, wherein the measuring step is carried out after the temporary storing step and uses the received recipient composition information to determine some of the bases of the second plurality of bases.
16. A method according to Claim 1, further comprising determining the second
20 plurality of bases independently of the first plurality of bases.
17. A method according to Claim 1, wherein the first and second pluralities of bases are selected randomly.
- 25 18. A method according to Claim 1, further comprising the recipient transmitting some information about the bases chosen for measurement and/or the measurement results to the sender.
19. A method according to Claim 1, wherein the step of carrying out the
30 reconciliation comprises using several quantum states to generate a single bit of the shared secret key at both the sender and recipient.

20. A method according to Claim 1, further comprising transmitting data regarding the second statistical distribution from the recipient to the sender.
21. A method according to Claim 1, further comprising determining the size of the secret shared key to be of the same order as the size of a message to be encrypted with the key.
22. A method according to Claim 1, wherein each of the plurality of random quantum states define two-dimensional information describing the condition of the quantum entity.
23. A method according to Claim 1, wherein each of the plurality of random quantum states define n-dimensional information describing the condition of the quantum entity, where n is three or more.
24. A method according to Claim 1, wherein the plurality of random quantum states are arranged geometrically to be uniformly separated within Hilbert space.
25. A secure communications method for conveying a message from a sender to an intended recipient, the method comprising:
- establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel according to a method as described in any preceding claim;
 - using the shared secret key as a one-time pad for secure encryption of the elements of the message at the sender;
 - transmitting the encrypted message to the intended recipient using a conventional communications channel; and
 - using the shared secret key as a one-time pad for secure decryption of the encrypted elements of the message at the recipient.
26. A method of a sender establishing a secret random cryptographic key shared with a recipient using a quantum communications channel, the method comprising:

generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space;

transmitting the plurality of random quantum states of the quantum entity via
5 the quantum channel to the recipient;

transmitting to the recipient composition information describing a subset of the plurality of random quantum states;

deriving a first binary string from the transmitted plurality of quantum states not in the subset; and

10 using error correction techniques to establish the shared secret random cryptographic key from the first binary string.

27. A method according to Claim 26, wherein the first plurality of bases in Hilbert space comprises at least four random bases.

15

28. A method according to Claim 26, wherein the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space.

20

29. A method according to Claim 26, wherein the selecting step comprises generating and measuring a first plurality of bases in a real subspace of two-dimensional Hilbert space.

25

30. A method according to Claim 26, wherein the composition information transmitting step comprises transmitting information describing the bases of the subset of the plurality of random quantum states.

30

31. A method according to Claim 26, wherein the subset information transmitting step comprises transmitting the subset information over a public channel, such as a radio channel.

32. A method according to Claim 26, wherein the quantum entity is photons and the quantum states are degrees of polarisation of the photons.

33. A method according to Claim 26, wherein the first plurality of bases is selected randomly.
- 5 34. A method according to Claim 26, wherein the step of using error correction techniques comprises using several quantum states to generate a single bit of the shared secret key at the sender.
- 10 35. A method of a recipient establishing a secret random cryptographic key shared with a sender using a quantum communications channel, the method comprising:
- receiving a plurality of random quantum states of a quantum entity via the quantum channel from the sender;
 - measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a recipient's plurality of bases in Hilbert space;
 - receiving from the sender composition information describing a subset of the plurality of random quantum states;
 - analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states;
 - establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar;
 - deriving a recipient binary string from the received plurality of quantum states not in the subset; and
 - using error correction techniques to establish the shared secret random cryptographic key from the recipient binary string.
- 30 36. A method according to Claim 35, wherein the recipient's plurality of bases in Hilbert space comprises at least four random bases.

37. A method according to Claim 35, wherein the analysing step comprises analysing the information describing the bases to derive the first statistical distribution.
- 5 38. A method according to Claim 35, wherein the establishing step comprises determining a statistical error rate.
39. A method according to Claim 35, wherein the establishing step comprises:
determining the degree of difference between the first and second statistical
10 distributions; and
accepting the security of the channel if the degree of correlation between the two distributions is greater than a threshold level.
40. A method according to Claim 39, further comprising selecting the value of the
15 threshold level.
41. A method according to Claim 35, wherein the deriving step comprises transmitting information to the recipient representing the bases for the quantum states not in the subset which make up the first binary string.
20
42. A method according to Claim 35, wherein the carrying out the reconciliation step comprises using privacy amplification techniques.
43. A method according to Claim 35, wherein the quantum entity is photons and
25 the quantum states are degrees of polarisation of the photons.
44. A method according to Claim 35, further comprising temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step.
30
45. A method according to Claim 44, wherein the measuring step is carried out after the temporary storing step and uses the received recipient composition information to determine some of the bases of the second plurality of bases.

46. A method according to Claim 35, wherein the recipient's plurality of bases is selected randomly.
- 5 47. A method according to Claim 35, further comprising the recipient transmitting some information about the bases chosen for measurement and/or the measurement results to the sender.
48. A method according to Claim 35, wherein the step of using error correction
10 techniques comprises using several quantum states to generate a single bit of the shared secret key at the recipient.
49. A method according to Claim 35, further comprising transmitting data
regarding the second statistical distribution from the recipient to the sender.

5